## REMARKS

Claims 1, 15-18, 34-36, 38 and 54 have been amended. Claims 37 and 53 have been canceled. Claims 1-36, 38-52 and 54 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

**Section 102(b) Rejection:**

The Examiner rejected claims 1-16, 18-33 and 35-53 under 35 U.S.C. § 102(b) as being anticipated by Hoover (U.S. Patent 6,209,102). Applicant respectfully traverses the rejection for at least the following reasons.

Regarding claim 1, Hoover fails to disclose *transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the response prior to said transmitting.* Hoover describes a system for hiding user input (e.g., PIN numbers or passwords) by displaying pseudo-randomized characters and allowing the user to change (e.g., increment and decrement) the characters until the access code is displayed. Column 3, lines 16-19 state, "Based on the display, the user provides feedback (in the form of an entered access code) via input device 340, which is passed back through processor 320 to access control program 350." Applicant asserts that Hoover passes the actual access code (i.e., password) to local processor 320 for validation. The Applicant's claim requires transmitting the response (e.g., the transformation of the challenge) received from the user input device to a remote authorization unit without including the pass code and without even generating the pass code.

Hoover also discloses sending the PIN in an Internet environment. Column 3, lines 30-40 states,

> In an Internet environment, the user-selectable fields could be implemented (i) using Javascript on a web page to send the PIN to a common gateway interface (CGI) script or active server page, (ii) using a Java applet on a web page to send the PIN to a CGI script or active server page, (iii) using a plug-in with a GUI on a

> web page to send the PIN to a CGI script or active server page, (iv) using a specialized network application with a GUI to send results by a network connection to a server application, or (v) using a specialized network application with command line input.

Thus, Hoover clearly sends the actual PIN (or pass code) in all embodiments. In contrast, Applicant's claim requires that the response be sent without the pass code and without generating the pass code from the response.

Claims 18, 35 and 38 include limitations similar to claim 1, and so the arguments presented above apply with equal force to these claims as well.

In regard to claim 36, Hoover does not teach receiving, from a user-input device, user input that transforms the challenge into a pass code allocated to the user, wherein the user input is dependent on the challenge such that the user input to transform the challenge into the pass code is different for different challenges; generating a response to the challenge from the user input received from the user input device wherein the response is not the pass code; generating a predicted response based on knowledge of the challenge and a stored version of the pass code; and validating the user on the basis of said user's response against the predicted response. As discussed above, the actual password or PIN is used for validation in Hoover, not a predicted response.

**Section 103(a) Rejections:**

The Examiner rejected claims 17, 34 and 54 under 35 U.S.C. § 103(a) as being unpatentable over Hoover in view of Funk (U.S. Patent 5,721,779). Applicant respectfully traverses the rejection for at least the following reasons.

Regarding claim 17, Hoover in view of Funk fail to disclose, *using the response to encrypt said communications challenge; and transmitting the encrypted communications challenge to the authorisation unit; thereby allowing the response to be validated by said authorisation unit against using said stored data record of, the pass code*. Hoover fails to teach the limitations of claim 1 (which claim 17 is dependent on)

for the reasons described above in the §102 remarks. The Examiner admits Hoover fails to teach using the response to encrypt the communications challenge and relies on Funk. The Examiner sites column 4, lines 50-52. Funk is directed towards utilizing a challenge and response handshake to allow a server to authenticate a client based on a password. Column 4, lines 50-53 state, "The client can generate this response signal by employing the same one-way commutative function to encrypt the challenge signal, C, with one valid password." Funk uses the password to generate the response. Column 4, line 59 provides the following formula: Response=$F(C,$ Password)=$C^{\text{password}}$ mod q. The Applicant's claim requires using the response (e.g., transformation of the challenge), not the pass code, to encrypt the communications challenge. Funk uses the actual password. Thus, Funk combined with Hoover would not result in Applicant's claimed invention.

In regard to the rejections under both § 102(b) and § 103(a), Applicant also asserts that the rejection of numerous ones of the dependent claims is further unsupported by the cited art. However, since the rejection of the independent claims has been shown to be improper, a further discussion of the rejection of the dependent claims is not necessary at this time.

## CONCLUSION

Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5681-74900/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicant

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: April 8, 2008